CLAIMS

1. A method of monitoring digital information including:

creating a secure wrapper around the digital information using a method selected from:

a first wrapper method including directly embedding a first executable protection software portion in the digital information; or

a second wrapper method including linking a second executable protection software portion to the digital information by way of an application program interface (API); or

a third wrapper method including modifying the digital information and embedding a third executable protection software portion in the modified digital information;

each of the first, second and third executable protection software portion including a specific performance portion operable by a user to perform one or more specific performance tasks, the or at least one of the specific performance tasks including a hardware environment check;

selecting one of the first second or third wrapper methods according to the software and development platform of the digital information, the accessibility of the source code of the digital information, and/or the level of monitoring required;

executing selected wrapper method by way of the first, second or third executable protection software portions including the steps of:

intercepting access to the digital information;

checking that at least one of the specific performance tasks has been performed, including the hardware environment check has been performed; and

validating whether or not the hardware environment corresponds to the hardware environment which has been previously checked.

2. A method according to Claim 1, wherein once the monitoring has been or is being performed, access to the digital information is provided in a manner transparent to the user that the digital information has been or is being monitored.

3. A method of monitoring digital information including:

creating a secure wrapper around the digital information by embedding an executable protection software portion in the digital information, the executable protection software including a specific performance portion operable by a user to perform one or more specific performance tasks, the or at least one of the specific performance tasks including a hardware environment check;

the secure wrapper being operable to:

intercept access to the digital information;

check that at least one of the specific performance tasks, including the hardware environment check has been performed; and

validate whether or not the hardware environment corresponds to the hardware environment which has been previously checked.

4. A method of monitoring digital information including:

creating a secure wrapper around the digital information by including linking an executable protection software portion to the digital information by way of an application program interface (API), said executable protection software portion including a specific performance portion operable by a user to perform one or more specific performance tasks, the or at least one of the specific performance tasks including a hardware environment check;

the secure wrapper being operable to:

intercept access to the digital information;

check that at least one of the specific performance tasks, including the hardware environment check has been performed; and

validate whether or not the hardware environment corresponds to the hardware environment which has been previously checked.

5. A method according to any one of Claims 1 to 4, wherein one of the specific performance tasks includes checking whether an operating system is operating having multiple virtual storage and a system user account check is performed instead of the hardware environment check, whereupon the remainder of the method uses the user account information instead of the hardware environment check.

6. A method of monitoring digital information including:

creating a secure wrapper around the digital information by modifying the digital information and embedding an executable protection software portion in the modified digital information;

the executable protection software including a specific performance portion operable by a user to perform one or more specific performance tasks, the or at least one of the specific performance tasks including a hardware environment check;

the secure wrapper being operable to:

intercept access to the digital information;

check that at least one of the specific performance tasks has been performed, including the hardware environment check has been performed; and

validate whether or not the hardware environment corresponds to the hardware environment which has been previously checked.

7. A method according to any one of the preceding claims, wherein the specific performance includes an exchange of codes between a client computer and a server computer operatively connected to the server computer.

8. A method according to Claim 7, wherein the exchange of codes includes:

the uploading of a code corresponding to the hardware environment of the client computer;

the uploading of a code corresponding to the digital information, such as, for example, a unique serial number or the like issued for that particular example of digital information; and

the downloading of a code corresponding to a key for entry into the client computer for accessing the digital information on an ongoing basis or for a selected countable unit.

9. A method of monitoring digital information in the form of a non-executable, browser-readable code and/or content including:

creating a mapping table capable of translating and preserving text, all object paths, extensions and such like within a single container or file structure to form a mapped file;

converting the mapped file into an executable file structure to form a conversion file;

encrypting the conversion file to form an encrypted file

embedding protection software as herein described to enable dynamic decryption of selected content of the encrypted file when correctly registered.

10. A system architecture for providing monitoring of digital information, including:

primary web server means for serving a computer network;

a plurality of client computers operatively connected to the primary web server means by way of the network;

one or more registration server means operatively connected to the primary web server and operatively connectible to the client computers by way of the network;

registration support means operatively associated with the primary web and registration server means for supporting the functionality of the primary web and registration server means;

wherein the primary web server means is operable to provide validation of a call from any client computer, tracking the client computer and if required redirecting the call;

and wherein the registration server means is operable to provide registration of each client computer when operatively connected thereto by way of the network;

the operative association of the registration support means including alternative means of communicating information between the client computers and the registration server means for client computers which are not connected thereto and the registration support means being operable to provide or functional in providing for registration of any client computer by way of the alternative means of communicating.

11. A system architecture according to Claim 10, further including data analysis means operatively connected to the registration server means for analysing the registration, usage or other billing, behavioural, demographic and/or market analysis of information received from the client computers in the registration and usage of digital information.

12. A method of protecting software, the method insofar as the installation and registration of the software including the steps of:

installing the software on a computer;

after installing the software, running the software for a first time;

upon the running of the software on the computer, generating an installation code from the hardware profile of the computer;

after generating the installation code, requesting a unique serial number from an authorisation source, the request including providing the hardware profile of the computer;

after requesting the serial number, registering the software with a registration authority using the serial number and installation code;

receiving a positive or negative reply from the registration authority;

upon the receipt of a negative reply from the registration authority, returning to the step of requesting a serial number and following the steps thereafter;

upon the receipt of a positive reply from the registration authority, receiving a registration key from the registration authority and saving the registration key on the computer, whereupon the software may be executed insofar as its functional performance is concerned;

the method insofar as the post-registration running of the software including the further steps of:

running the software on the computer;

upon the running of the software on the computer, generating an installation code from the hardware profile of the computer;

after the hardware profile has been generated, comparing the registration key with the hardware profile;

upon the matching of the hardware profile with the registration key, permitting the software to executed insofar as its functional performance is concerned;

upon the failure of the hardware profile to match the registration key, denying permission for the software to executed insofar as its functional performance is concerned.

13. A method of monitoring digital information including:

adding a protection software portion;

modifying the protection software portion so as to mask its identifying characteristics and behaviour. For example, operative portions of program code may be embedded into other code which is, apparently, functional, but never called by the actual program in its operation.

14. A method of monitoring digital information having a protection software portion as hereinbefore described, including;

adding a specific performance portion for checking for the presence of code-breaking methods;

checking for the presence of code-breaking methods to provide a check result; and

modifying the behaviour of the protection software portion in accordance with the check result.